Draft Implementing Rules under the Personal Data Protection Act 2019

Comments from BSA | The Software Alliance

May 19 2022

Introduction

BSA | The Software Alliance (**BSA**)[1] welcomes this opportunity to provide our comments to the Office of the Personal Data Protection Committee (**PDPC Office**) regarding the draft Implementing Rules under the Personal Data Protection Act (**PDPA**). BSA is the leading advocate for the global software industry before governments and in the international marketplace. We have extensive experience engaging with governments around the world to promote effective, internationally interoperable legal systems that protect personal information and provide strong consumer rights while supporting responsible uses of data-driven technologies.

BSA members create the technology products and services that power other businesses. Our members offer tools including cloud storage services, customer relationship management software, human resources management programs, identity management services, security solutions, and collaboration software. BSA members are enterprise software companies that are in the business of providing privacy protective technology products and services and, their business models do not depend on monetizing users' data. Companies entrust some of their most sensitive information to BSA members. Our members recognize that companies need to earn consumers' trust and act responsibly with their personal data, and BSA members work hard to keep that trust. We also support an internationally interoperable approach to data protection that enables companies to deliver global services that benefit the individuals and businesses they serve, creating local jobs and adding value to the Thai economy.

As enterprise software companies, BSA members generally act as data processors under the PDPA because they handle data on behalf of their business customers, which act as data controllers. Our comments accordingly focus on measures designed to ensure data processors protect personal data.

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Aveva, Bentley Systems, Box, Cisco, CNC/Mastercam, Dassault, DocuSign, Dropbox, IBM, Informatica, Intel, MathWorks, Microsoft, Nikon, Okta, Oracle, PTC, Rockwell, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

300 Beach Road
#30-06 The Concourse
Singapore 19955

P +65 6292 2072
F +65 6292 6369
W bsa.org

Regional Representative Office
UEN: S97RF0005K

Below, we make two recommendations on the draft Implementing Rules:

- First, for the Implementing Rules on **Records of Processing Activities for Personal Data Processors**, we recommend ensuring that record keeping requirements for data processors are in line with the record keeping obligations of data processors under global privacy frameworks such as the General Data Protection Regulation (**GDPR**), as well as common contractual obligations; and

- Second, for the Implementing Rules on **Security Measures for Personal Data Controllers**, we recommend the rules avoid applying controller-facing data security obligations to data processors, which may not fit their distinct role.

Recommendations

I. Records of Processing Activities for Personal Data Processors: Requirements Should Be Aligned with Data Processors' Contractual Obligations

BSA is concerned with the proposed requirements under **Article 3(4) and (5) of the draft Implementing Rules for Records of Processing Activities for Personal Data Processors.** These provisions require data processors to maintain records on the:

- "*type or nature of the collection, use, or disclosure of personal data that the data processor acts on instruction of or on behalf of the data controller, including personal data and the purposes for which it is collected, used, or disclosed as assigned by the data controller*" (Article 3(4)); and,

- "*type of person or agency receiving personal data in the event that personal data is sent or transferred to a foreign country*" (Article 3(5)).

At the outset, we want to reiterate our support for the clear distinction between data controllers and data processors contained in the PDPA. A comprehensive data protection framework must create effective and enforceable obligations for all companies that handle consumer data, but these obligations will only be effective in protecting consumer privacy and instilling trust if they reflect how a company interacts with consumer data. The distinction between data controllers and data processors is paramount because both data controllers and data processors have important, but different, roles in processing and protecting personal information.

We are concerned that Articles 3(4) and (5) of the draft implementing rules may be read in a manner that distorts the important relationship between data processors and their customers, the data controllers. As the PDPC Office develops implementing rules to ensure that data processors remain accountable for handling personal data securely, it is important that the rules take into account the unique role data processors play vis-à-vis data controllers and do not assign them obligations that do not fit their role as a provider of services to other businesses.

As written, Article 3(4) and Article 3(5) may both require data processors to keep records of information that they are not privy to, given their limited role in processing data on behalf of, and on the instruction of, other companies. For example, data processors may have only limited information about the nature of the data they are processing and the purposes for which such processing is being conducted — because it is the data controller (rather than the processor) that determines which types of data to collect and the purpose for which that data will be processed.

Moreover, data processors are typically subject to contractual and technical limits on accessing data they store or otherwise process for a controller and often design their services to minimize the amount of personal data they can or need to access — all of which better protects the privacy of that data. Requiring data processors to access and maintain records of personal data they otherwise would not, risks undermining such protections.

Article 3(4)'s requirement to keep records about the "personal data and the purposes for which it is collected, used, or disclosed as assigned by the data controller" may require processors to keep records of information they do not have – because it is the data controller that determines the purposes for collecting, using and disclosing such data. To the extent Article 3(4) is retained, we recommend focusing it on requiring data processors to keep records of the data types and processing activities set out in the contract between a data processor and a controller, rather than requiring the data processor to create new records of information it may not have access to.

Article 3(5)'s requirement to keep records about the "type of person or agency receiving personal data" for data transferred outside Thailand raises similar concerns. We recommend either interpreting this provision to require data processors to only keep such records in relation to its own sub-processors in third countries, and/or allowing data processors to satisfy this obligation by retaining documentation of data transfers agreed to as between a controller and data processor in the contract. This may help to avoid situations in which a processor could be required to keep records of activities it does not have information about, such as when an individual user of the controller initiates a transfer to a third country.

Specifically, BSA recommends that Article 3(4) and (5) be amended as follows:

> ***(4)*** *Types of personal data and purposes of processing set out in the contract between a controller and a processor*
>
> ***(5)*** *Where applicable, documentation of data transfer as set out in the contract between a controller and processor*

II. Security Measures for Personal Data Controllers: Avoid Applying Controller-Facing Data Security Obligations to Data Processors, Given Their Distinct Role

BSA recognizes the importance of safeguarding personal information and supports requirements for companies to adopt reasonable security measures designed to protect personal information. The PDPA adopts this obligation in Sections 37(1) and 40(2), under which both personal data controllers and data processors are required to put in place "appropriate security measures" to prevent the unlawful loss, access, use, modification, editing, or disclosure of personal data.

We are concerned that Article 6 of the draft Implementing Rules for Security Measures for Personal Data Controllers extends these obligations to data processors in a manner that distorts the relationship between a data processor and its customers, the data controllers. In particular, Article 6 requires data processors to meet "minimum security measure requirements" outlined in Article 4, which creates data security obligations for data controllers. However, Article 4 is drafted to apply to data controllers – which make decisions regarding the collection, use, or disclosure of personal information – and were not drafted to fit the distinct role of data processors. For example, several aspects of Article 4(6) raise concerns when applied to data processors –

because those requirements are to be applied considering the nature and purposes of the collection and use of the personal data at issue. Extending these controller-facing obligations to data processors could inadvertently undermine the privacy and security of personal data intended to be protected by the PDPA. Moreover, Article 40(2) of the PDPA already requires data processors to provide appropriate security measures.

It is also important for the PDPC Office to allow data controllers and data processors the flexibility to negotiate agreements that befit the type(s) of data entrusted to the data processor for processing, and the protections that need to be accorded to such data. To this end, we recommend amending Article 6 as follows:

> ***(4)*** A data processor shall provide security measures to ensure that the data controller can comply with its obligations as outlined in Article 4, taking into account *the nature of processing and the information available to the data processor*

Conclusion

BSA appreciates the opportunity to provide our comments and recommendations on the draft Implementing Rules of the PDPA. We support the Government of Thailand's efforts in implementing the PDPA successfully and look forward to continuing working with the Ministry of Digital Economy and Society and the Office of the Personal Data Protection Committee on privacy and personal data protection policies. Please do not hesitate to contact the undersigned at eunicel@bsa.org if you have any questions or comments regarding our suggestions.

Yours faithfully,

Eunice Lim

Eunice Lim

Senior Manager, Policy – APAC

BSA | The Software Alliance